ABSTRACT

A method and apparatus are disclosed for preventing noise from influencing a random number generator that is based on the meta-stable behavior of flip-flops. External noise will affect multiple flip-flops in a larger random number generator circuit in the same way, since they are physically close. Thus, the ability to influence the operation of a random number generator using external noise is reduced by incorporating a plurality of flip-flops, referred to herein as core random elements, in a single random number generator. If one of the core random elements in a random number generator is influenced by noise, all of the core random elements will be influenced by the noise. Thus, if all (or most) of the core random elements issue a random bit at the same time, there is a possibility that the random number generator was influenced by noise, and all the issued bits are discarded. One or more mechanisms are incorporated into the random number generator to ensure that a random bit is not generated when a plurality of the core random elements generate a bit at the same time.